Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP

Devi Anjheli
UIN Sunan Kalijaga Yogyakarta
E-mail: devianjheli@gmail.com

Abstract: *The rapid development of information technology has given rise to new and increasingly complex challenges, one of which is phishing. This study aims to evaluate the legal aspects of data breaches caused by phishing in Indonesia and assess the effectiveness of existing regulations in protecting users' digital privacy rights. Using a normative juridical approach and descriptive qualitative method, this research reveals that current regulations, such as the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP), do not comprehensively or specifically address the elements of phishing crimes, particularly in the form of malicious APK files. The 2001 phishing case involving Bank Central Asia's internet banking service is presented as a historical benchmark for analyzing the weaknesses in Indonesia's legal framework. The findings show that phishing leads not only to financial loss but also to serious repercussions on users' reputations, privacy rights, and data security. This study recommends the formulation of a specific regulation on phishing, stronger enforcement of the PDP Law, and enhanced public digital literacy and cybersecurity emergency response systems. The limitation of this study lies in the lack of empirical data from victims or law enforcement authorities; thus, further interdisciplinary and field-based research is highly recommended.*
Keywords: *phishing; data breach; digital privacy; cyber law; ITE Law; PDP Law.*

Abstrak: Perkembangan teknologi informasi telah melahirkan tantangan baru dalam bentuk kejahatan siber yang kian kompleks, salah satunya adalah phishing. Penelitian ini bertujuan untuk mengevaluasi aspek hukum dari kebocoran data akibat phishing di Indonesia serta menelaah efektivitas regulasi yang ada dalam menjamin hak atas privasi digital pengguna. Dengan menggunakan pendekatan yuridis-normatif dan metode kualitatif deskriptif, penelitian ini menemukan bahwa regulasi seperti UU ITE dan UU PDP belum secara spesifik dan komprehensif mengatur unsur-unsur tindak pidana phishing, khususnya dalam modus melalui file aplikasi (APK). Studi kasus serangan phishing terhadap layanan internet banking BCA tahun 2001 menjadi titik tolak analisis historis tentang lemahnya kerangka hukum nasional. Temuan juga menunjukkan bahwa phishing tidak hanya menyebabkan kerugian finansial, tetapi juga berdampak serius

terhadap reputasi, hak privasi, dan keamanan data pengguna. Rekomendasi penelitian ini mencakup perlunya pembentukan regulasi khusus mengenai phishing, penguatan penegakan UU PDP, serta peningkatan literasi digital dan sistem tanggap darurat keamanan siber. Keterbatasan penelitian ini terletak pada minimnya data empiris langsung dari korban atau aparat penegak hukum, sehingga disarankan untuk dilakukan studi lanjutan yang bersifat interdisipliner dan berbasis lapangan.
Kata kunci: *phishing; kebocoran data; privasi digital; hukum siber; UU ITE; UU PDP.*

Pendahuluan

Perkembangan teknologi informasi dan komunikasi (TIK), dalam dua dekade terakhir, telah merevolusi cara manusia berinteraksi, bertransaksi, dan mengakses informasi di seluruh dunia.[1] Internet, yang semula dikembangkan dalam ruang lingkup terbatas seperti lembaga akademik dan militer, kini telah menjadi ruang publik global yang melampaui batas-batas geografis dan yurisdiksi.[2] Di Indonesia, pertumbuhan pengguna internet terus menunjukkan tren peningkatan. Berdasarkan laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2023, lebih dari 215 juta penduduk telah terhubung dengan internet, mencerminkan transformasi digital yang masif dan menyentuh hampir seluruh aspek kehidupan masyarakat, mulai dari komunikasi, pendidikan, hingga sektor perbankan dan perdagangan elektronik.[3]

Namun, kemajuan ini tidak datang tanpa konsekuensi. Ruang siber yang luas dan dinamis telah membuka peluang besar bagi lahirnya kejahatan berbasis digital atau yang dikenal sebagai cybercrime.[4] Di

[1] Ye Zhipeng, "The Social Impact of the Evolution of Internet Language: A Critical Discourse Analysis of Popular Internet Language," *Lecture Notes on Language and Literature* 7, no. 2 (2024), https://doi.org/10.23977/langl.2024.070223.

[2] Thompson S.H. Teo, "Differential Effects of Occupation on Internet Usage," *Internet Research* 8, no. 2 (1998): 156–65, https://doi.org/10.1108/10662249810211629.

[3] Agus Tri Haryanto, "APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang," detiknet, 2024, https://inet.detik.com/cyberlife/d-7169749/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang.

[4] Miranda Bruce et al., "Mapping the Global Geography of Cybercrime with the World Cybercrime Index," *PLoS ONE* 19, no. 4 April (2024), https://doi.org/10.1371/journal.pone.0297312.

antara berbagai bentuk kejahatan siber, phishing menempati posisi yang mengkhawatirkan karena sifatnya yang tersembunyi dan manipulatif, serta dampaknya yang signifikan terhadap kerahasiaan dan keamanan data pribadi.[5] Phishing merujuk pada tindakan penipuan yang bertujuan untuk memperoleh informasi sensitif seperti username, password, atau data kartu kredit dengan cara menyamar sebagai entitas tepercaya dalam komunikasi elektronik. Fenomena ini tidak hanya mengancam privasi pengguna tetapi juga mengganggu stabilitas sistem keuangan dan menurunkan kepercayaan publik terhadap layanan digital.[6]

Salah satu kasus phishing yang paling mencolok di Indonesia terjadi pada tahun 2001, ketika para pelaku berhasil menciptakan situs palsu yang menyerupai tampilan resmi dari layanan perbankan daring Bank Central Asia (BCA), yaitu klikbca.com. kasus phishing terhadap layanan internet banking Bank Central Asia (BCA) pada tahun 2001 sering dianggap sebagai salah satu insiden phishing pertama yang signifikan di Indonesia.[7] Dengan membeli domain-domain serupa, pelaku berhasil menipu nasabah dan merekam data-data login mereka. Kejadian ini menjadi titik awal kesadaran nasional akan pentingnya regulasi dan perlindungan hukum di ranah siber. Seiring dengan meningkatnya jumlah insiden kebocoran data dan eksploitasi digital, pemerintah Indonesia meresponsnya dengan merumuskan kebijakan hukum seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008, serta Peraturan Pemerintah Pengganti Undang-Undang (Perppu) dan regulasi turunannya.[8]

Secara umum, isu kebocoran data pribadi telah menjadi perhatian utama berbagai negara dan organisasi internasional. Penelitian oleh Anderson dkk. (2019) mengindikasikan bahwa kerugian

---

[5] Kevin F. Steinmetz et al., "Exploring Cybercrime Capabilities: Variations Among Cybercrime Investigative Units," *Criminal Justice Policy Review* 35, no. 4 (2024): 194–215, https://doi.org/10.1177/08874034241265106.

[6] Mohd Yusuf Dm, Addermi, and Jasmine Lim, "Kejahatan Phising Dalam Dunia Cyber Crime Dan Sistem Hukum Di Indonesia," *Jurnal Pendidikan Dan Konseling* 4, no. 5 (2022): 8018–23.

[7] Muftiadi A, Putri Mulyani Agustina T, and Evi M, "Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phising Terhadap Layanan Online Banking," *HEXATECH Jurnal Ilmiah Teknik* 1 (2022).

[8] Handika Saputra Harahap et al., "Memahami Cara Kerja Phishing Menggunakan Tools Pada Kali Linux," *Journal of Internet and Software Engineering* 1 (2024): 1–11.

akibat serangan siber, termasuk phishing, telah mencapai miliaran dolar per tahun secara global.[9] Sementara di Indonesia, Lembaga Riset Siber CISSReC mencatat setidaknya 98 juta data pribadi bocor ke publik antara 2020 hingga 2022, yang sebagian besar berasal dari sektor keuangan, e-commerce, dan pemerintahan.[10] Situasi ini menunjukkan bahwa perlindungan data pribadi dan privasi digital bukan hanya isu teknologi, tetapi telah menjadi problematika hukum dan sosial yang kompleks dan mendesak.[11]

Berbagai studi sebelumnya telah mengeksplorasi dinamika kejahatan siber dalam konteks internasional seperti David S. Wall (2024) dan Grabosky (2016) maupun di Indonesia Yuspin dkk. (2024). Wall berargumen bahwa kejahatan siber tidak sekadar perluasan dari bentuk kriminalitas konvensional ke ranah daring, tetapi telah membentuk kategori kriminalitas baru yang bersifat transformasional yang mana struktur dan modus operandi dari kejahatan di dunia maya memiliki logika tersendiri, pelaku memanfaatkan karakteristik anonim, terdistribusi, dan borderless dari internet untuk melakukan penipuan, pencurian data, dan serangan terhadap infrastruktur digital.[12] Lebih lanjut, Grabosky juga menjelaskan bagaimana bentuk kejahatan siber seperti phishing dan kebocoran data pribadi tidak hanya menantang norma hukum yang ada, tetapi juga menuntut perubahan paradigma dalam penegakan hukum dan kebijakan publik. Grabosky memperkenalkan pendekatan multidisipliner dalam memahami cybercrime, menggabungkan perspektif hukum, teknologi, kriminologi, dan kebijakan. Ia juga menekankan pentingnya respons kolektif antara negara, sektor swasta, dan masyarakat sipil untuk menghadapi eskalasi

[9] Ross Anderson et al., "Measuring the Changing Cost of Cybercrime," in *Workshop on the Economics of Information Security*, 2019, https://doi.org/https://doi.org/10.17863/CAM.41598.

[10] Bianda Ludwianto, "91 Juta Data Pengguna Tokopedia Yang Bocor Beredar Gratis Di Facebook," 2020, https://kumparan.com/kumparantech/91-juta-data-pengguna-tokopedia-yang-bocor-beredar-gratis-di-facebook-1tkItz2vI05?; Rita Puspita Sari, "RI Masuk 10 Besar Kebocoran Data, Hampir 100 Juta Akun Bocor," 2024, https://csirt.or.id/berita/ri-masuk-10-besar-kebocoran-data?

[11] C Desai and V P Desai, "Ensuring Data Security in Human Resource Management: Importance, Challenges \&Techniques," in *Sdmimd.Ac.In*, n.d., https://www.sdmimd.ac.in/conferenceproceedings/ihr2024papers/IHR2418.pdf.

[12] David S. Wall, "Cybercrime: The Transformation of Crime in the Information Age, 2nd Edition, Cambridge: Polity (Outline of Update)," *SSRN Electronic Journal*, 2024, https://doi.org/10.2139/ssrn.4707509.

ancaman digital yang bersifat lintas batas.[13] Penelitian Yuspin dkk. (2024) berfokus pada aspek teknis dalam kerangka hukum, dengan menyoroti kerentanan sektor perbankan digital terhadap serangan phishing. Studi ini mengungkap bahwa phishing di Indonesia sering menyasar pengguna layanan perbankan daring melalui berbagai skema, seperti peniruan situs resmi maupun panggilan palsu yang mengatasnamakan institusi keuangan.[14] Namun, kajian yang secara khusus memfokuskan pada keterkaitan antara praktik phishing, kebocoran data, dan analisis regulasi hukum nasional masih relatif terbatas. Beberapa penelitian lebih banyak menyoroti aspek teknis atau kebijakan umum, tetapi belum secara mendalam menelaah bagaimana kebocoran data akibat phishing berdampak terhadap perlindungan hak privasi individu dalam kerangka hukum positif Indonesia. Gap ini menunjukkan adanya kebutuhan mendesak untuk mengkaji efektivitas dan kecukupan regulasi yang ada, serta bagaimana regulasi tersebut diterapkan dalam menangani kasus-kasus konkret.

Penelitian ini bertujuan untuk mengevaluasi aspek hukum dari fenomena kebocoran data akibat phishing di Indonesia, dengan menelaah sejauh mana regulasi yang ada, terutama UU ITE dan peraturan terkait perlindungan data pribadi, mampu menjawab tantangan-tantangan kontemporer dalam dunia siber. Fokus utama diberikan pada pemahaman terhadap implikasi hukum atas pelanggaran privasi pengguna, serta bagaimana norma dan prinsip perlindungan hak asasi manusia, khususnya hak atas privasi, diposisikan dalam kebijakan siber nasional.

Secara metodologis, penelitian ini menggunakan pendekatan yuridis-normatif dengan metode kualitatif deskriptif. Data dikumpulkan melalui studi pustaka terhadap peraturan perundang-undangan UU ITE dan UU PDP, serta analisis kasus yang relevan. Selain itu, digunakan pula data sekunder dari laporan media, hasil riset lembaga nonpemerintah, serta literatur akademik untuk memperkaya interpretasi.

---

[13] Peter Grabosky, *Cybercrime*, ed. Henry N. Pontell (Oxford University Press, 2015).

[14] Wardah Yuspin et al., "Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities," *International Journal of Safety and Security Engineering* 14, no. 6 (2024), https://doi.org/10.18280/ijsse.140605.

Dengan mempertimbangkan urgensi isu dan kesenjangan riset yang telah disebutkan, penelitian ini dirancang untuk menjawab dua pertanyaan utama: (1) Bagaimana karakteristik kasus kebocoran data akibat phishing di Indonesia, dan bagaimana praktik tersebut diproses dalam kerangka hukum Indonesia? (2) Sejauh mana regulasi perlindungan data pribadi dan kebijakan siber di Indonesia telah efektif dalam menjamin hak atas privasi digital pengguna?

Hasil dan Pembahasan

Kasus Phishing Pertama di Indonesia dan Perkembangannya: Kajian atas Serangan KlikBCA dan Dampaknya

Perkembangan kebutuhan masyarakat dewasa ini tidak dapat dilepaskan dari peran sentral teknologi informasi yang terus mengalami transformasi signifikan.[15] Dinamika teknologi, khususnya dalam bidang informasi dan komunikasi, tidak hanya memengaruhi cara manusia berinteraksi dan mengakses layanan, tetapi juga secara mendasar mengubah pola kehidupan sosial, ekonomi, dan budaya masyarakat kontemporer. Internet, yang pada awalnya merupakan instrumen terbatas dalam lingkungan akademik dan militer, kini telah menjadi infrastruktur dasar dalam kehidupan sehari-hari. Akses terhadap internet bukan lagi sekadar fasilitas tambahan, melainkan telah menjelma sebagai kebutuhan esensial dalam tatanan masyarakat digital modern.[16] Kemudahan, kecepatan, dan konektivitas tanpa batas ruang dan waktu yang ditawarkan oleh internet mendorong terjadinya ketergantungan sosial yang masif terhadap ruang siber, melampaui batas-batas usia, geografis, bahkan identitas sosial.[17]

---

[15] Fabrício Sobrosa Affeldt and Sady Darcy da Silva Junior, "Information Architecture Analysis Using Business Intelligence Tools Based on the Information Needs of Executives," *Journal of Information Systems and Technology Management* 10, no. 2 (2013): 251–70, https://doi.org/10.4301/s1807-17752013000200004.

[16] Lucysera Sinaga, Oriza et al., "Pengaruh Perkembangan Teknologi Terhadap Pola Komunikasi Masyarakat," *JURNAL SIMBOLIKA Research and Learning in Comunication* 4, no. 2 (2021): 188–99, https://www.researchgate.net/publication/348408331_Pengaruh_Perkembangan_Teknologi_Terhadap_Pola_Komunikasi_Masyarakat.

[17] Anas R M Lubbad, "Information Technology Readiness and the Assessment and Adoption of Information Technology Innovativeness," *Advances in Life Science and Technology*, 2021, https://doi.org/10.7176/alst/90-04.

Seiring dengan akselerasi transformasi digital, media sosial juga mengalami pertumbuhan eksponensial, menjadi medium utama komunikasi lintas personal, institusional, hingga transnasional. Penggunaan media sosial telah mempermudah pertukaran informasi, memperluas ruang partisipasi publik, dan membuka peluang kolaboratif lintas sektor.[18] Namun demikian, sisi gelap dari ekspansi teknologi ini juga mulai tampak, terutama ketika platform digital disalahgunakan oleh oknum tertentu untuk kepentingan destruktif. Penyimpangan fungsi media sosial tersebut berkontribusi terhadap munculnya bentuk-bentuk kejahatan baru yang bersifat virtual dan tidak kasatmata, yang dalam ranah hukum dan kriminologi dikenal sebagai cybercrime.[19] Kejahatan ini mencakup segala aktivitas ilegal yang memanfaatkan jaringan komputer, baik untuk meretas sistem, menyebarkan informasi palsu, hingga mengeksploitasi data pribadi secara tanpa hak. Kejahatan siber, dengan segala kompleksitas teknologinya, kini menjadi ancaman global yang nyata terhadap keamanan informasi dan hak privasi individu dalam ekosistem digital.[20]

Dimulai dari kategori ringan seperti penyebaran virus, spam email, dan penyadapan transmisi, hingga kejahatan-kejahatan kategori berat seperti phishing. Phishing yang merupakan kependekan dari password harvesting fishing, adalah bentuk umum penipuan online yang melibatkan pengiriman email palsu yang mengaku berasal dari organisasi tepercaya atau menyamar sebagai entitas terpercaya di situs web yang sebenarnya asli untuk mendapatkan data pengguna.[21] Teknik umum phishing termasuk memalsukan email atau pesan instan, dan korban biasanya ditipu untuk menggunakan metode ini. Praktik penipuan ini berbentuk situs web yang seolah-olah berasal dari bisnis

[18] Varatisha Abdullah, "SOSIAL MEDIA SEBAGAI PASAR BAGI MASYARAKAT MODERN (Sebuah Kritik Terhadap Budaya Populer)," *Jurnal Dakwah Tabligh* 18, no. 1 (2017): 1–15, https://doi.org/10.24252/jdt.v18n1dnk02.

[19] Maskun, *Kejahatan Siber Cybercrime: Suatu Pengantar* (Jakarta: Kencana, 2013).

[20] Anjeli Holivia and Teguh Suratman, "Child Cyber Grooming Sebagai Bentuk Modus Baru Cyber Space Crimes," *Bhirawa Law Journal* 2, no. 1 (2021): 1–13, https://doi.org/10.26905/blj.v2i1.5847.

[21] Pedro Ramos Brandao and Henrique S Mamede, "Phishing and Advanced Persistent Threats," *Journal of Mathematical & Computer Applications*, 2022, 1–4, https://doi.org/10.47363/jmca/2022(1)105.

atau instansi pemerintah yang sah untuk mencuri informasi sensitif, seperti PIN, nomor rekening, nomor kartu kredit, dan lainnya.[22]

Salah satu bentuk kejahatan di dunia maya yang dilakukan oleh para penipuan adalah phishing. Phishing merupakan suatu aktivitas kriminal yang memanfaatkan teknik rekayasa sosial. Satuan Tugas Anti-Phishing melaporkan bahwa pada kuartal kedua tahun 2014, sektor layanan pembayaran menjadi target utama industri, dengan 39,80% dari total serangan yang terjadi dalam periode tiga bulan dari April hingga Juni 2014, sementara sektor layanan keuangan terus berada di belakang. Sektor keuangan menjadi salah satu sasaran eksploitasi para pelaku penipuan. Perbankan, sebagai layanan untuk transaksi keuangan secara massal, tidak luput dari ancaman para penipu siber. Phishing dapat dilakukan dengan menggunakan halaman web palsu yang menyamar sebagai situs resmi bank, dengan tujuan untuk menipu dan mencuri identitas pengguna.

Insiden phishing kian marak terjadi pada layanan perbankan online di bank-bank di Indonesia. Kepala Otoritas Jasa Keuangan melaporkan bahwa sejak tahun 2013, pengguna merugi hingga Rp 100 miliar akibat kasus pencurian dengan metode "phishing" (PT. Kompas Cyber Media, 2015). Pada tahun 2015, dua bank besar di Indonesia, yaitu Bank BCA dan Bank Mandiri, mengimbau agar penggunanya lebih berhati-hati saat bertransaksi melalui internet banking. Pengguna diminta untuk memahami pesan mengenai sinkronisasi token di situs web kedua bank, terutama jika mereka tidak melakukan transaksi apa pun di layanan "Internet banking". Serangan phishing tidak hanya mengakibatkan kerugian finansial, tetapi juga membawa konsekuensi serius berupa hilangnya data pribadi pengguna dan kerugian reputasi bagi perusahaan yang mereknya tercoreng akibat insiden phishing ini.[23]

Phishing pertama kali muncul pada tahun 1995. Metode awal yang dipakai oleh phisher adalah menggunakan algoritma untuk menghasilkan nomor kartu kredit secara acak. Sekumpulan nomor kartu kredit acak tersebut digunakan untuk membuat akun AOL. Akun itu kemudian dimanfaatkan untuk mengirim spam kepada pengguna

[22] Adhitya Widya Kartika Radya Dzuhrizha Rahmana, "Penegakan Hukum Bagi Pelaku Pembuatan Dan Penyebaran Scam Page (Studi Di Kepolisian Daerah Jawa Timur)," *Risalah Hukum* 2 (2022): 83–98.

[23] Koko Caniago and Tata Sutabri, "Tindak Kejahatan Phising Di Sektor Pelayanan Di Universitas Bina Insan Lubuklinggau," *Jurnal Riset Sistem Informasi Dan Teknik Informasi* 8, no. 1 (2023): 117–25.

lain dan untuk keperluan lainnya.[24] Untuk menyederhanakan proses ini digunakan program khusus seperti AOHell. Praktik semacam itu dihentikan oleh AOL pada tahun 1995 ketika perusahaan mulai menerapkan langkah-langkah keamanan untuk mencegah keberhasilan pemanfaatan nomor kartu kredit yang dihasilkan secara acak.[25] Phishing, yang juga dikenal dengan istilah *Brand Spoofing* atau *Carding*, merupakan bentuk layanan yang menipu target dengan mengklaim bahwa data target aman dan legal.[26] *Spoofing* dapat dijelaskan sebagai teknik yang digunakan untuk memperoleh akses tidak sah ke komputer atau informasi di mana penyerang berkomunikasi dengan pengguna dengan berpura-pura menjadi pihak yang dapat dipercaya.[27]

Pada tahun 2001, terjadi sebuah kasus pembobolan internet banking di Bank BCA yang melibatkan mantan mahasiswa ITB Bandung dan pegawai media internet dari satunet. com, yaitu Steven Haryanto. Menariknya, Steven bukanlah seorang insinyur listrik atau komputer, melainkan seorang insinyur kimia. Ide tersebut berawal ketika Steven secara tidak sengaja salah mengetik alamat situs web. Ia kemudian membeli sebuah domain internet senilai sekitar $20 yang menggunakan nama yang sering salah ketik oleh orang-orang dan tampil dengan sangat mirip seperti situs internet banking BCA.[28] Dia lalu membeli sebuah domain internet seharga sekitar $20 yang menggunakan nama yang sering salah ketik dan sangat mirip dengan situs internet banking BCA, seperti http://www. klikbca. com, contohnya: wwwklikbca. com, kilkbca. com, klikbca. com, klikbca. com, klikbac. com. Nasabah bank mungkin tidak menyadari bahwa mereka telah mengunjungi situs tersebut karena tampilannya yang menyerupai situs aslinya. Peretas bisa mengumpulkan ID pengguna dan kata sandi dari pengguna yang masuk ke dalam perangkat lunak, namun

[24] "History of Phishing," Phishing.org, accessed March 15, 2025, https://www.phishing.org/history-of-phishing?

[25] Adam Levy, *Avoiding the Ransom Cybersecurity for Business Owners and Managers* (Magnet Solution Group Press, 2016).

[26] Rohit Manglik, *Cybercrime, Law and Countermeasures* (EduGorilla Publication, 2024).

[27] Vaishnavi Bhavsar, Aditya Kadlak, and Shabnam Sharma, "Study on Phishing Attacks," *International Journal of Computer Applications* 182, no. 33 (2018): 27–29, https://doi.org/10.5120/ijca2018918286.

[28] Muftiadi A, Putri Mulyani Agustina T, and Evi M, "Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phising Terhadap Layanan Online Banking."

peretas tersebut tidak berniat melakukan tindakan kriminal seperti mencuri dana pelanggan, melainkan murni karena rasa ingin tahu tentang berapa banyak orang yang tidak sadar akan penggunaan klikbca. com serta untuk menguji tingkat keamanan situs tersebut.

Stephen Haryanto bisa dikategorikan sebagai hacker karena dia telah meretas sistem orang lain yang seharusnya dilindungi privasinya. Oleh karena itu, tindakan Steven ini disebut hacking. Steven dapat digolongkan sebagai tipe hacker yang merupakan kombinasi antara *white hat hacker* dan *black hat hacker*, yang mana ia hanya bertujuan untuk mengevaluasi seberapa aman situs internet banking Bank BCA. Ia disebut sebagai *white hat hacker* karena tidak mencuri dana nasabah, melainkan hanya mendapatkan user ID dan password nasabah yang dimasukkan di situs internet banking palsu. Namun, tindakan Steven juga mencakup karakteristik *hacker black hat* karena ia menciptakan website palsu untuk dengan diam-diam mengumpulkan data milik orang lain.[29] Steven memiliki kemampuan sebagai pemindai, sniffer, dan cracker kata sandi. Pelaku mengirimkan situs palsu melalui email dengan teks yang menyerupai situs aslinya. Jika pemilik akun tidak waspada, korban dapat mengklik situs palsu tersebut sesuai arahan pelaku, termasuk mengupdate akun mereka untuk informasi lebih lanjut mengenai data pribadi. Pemilik akun akan dialihkan kembali ke situs palsu yang telah mereka klik sebelumnya, memungkinkan penyerang untuk melakukan apa saja dengan informasi tersebut, termasuk mencuri rekening bank.

Saat menjebak mangsanya, phisher menggunakan beberapa teknik, antara lain:[30]

1. Email spoofing. Metode ini biasa digunakan oleh phisher untuk mengirim email ke jutaan pengguna dengan kedok institusi resmi. Biasanya, email berisi permintaan nomor kredit, kata sandi, atau formulir tertentu untuk diunduh.
2. Internet Submission. Internet Submission adalah salah satu metode phishing yang paling canggih. Peretas juga dikenal sebagai "manusia di tengah", berada di antara situs web

[29] Bishal Poudel and Satish Kumar Karna, "What Influences a Hacker to Be a Black Hat?," *Medicon Engineering Themes*, 2024, https://doi.org/10.55162/mcet.06.215.

[30] Eko Jhony Pranata and Lukman Ependi, "Phising Terhadap Website Bank Bca," *Jurnal Trends* 01, no. 01 (2023): 34–40, https://ejurnal.ibisa.ac.id/index.php/jsd/article/view/293.

sebenarnya dan sistem phishing.

3. Pesan instan (obrolan). Pesan instan adalah metode di mana pengguna menerima pesan dengan tautan yang mengarahkan mereka ke situs web phishing palsu yang terlihat seperti situs asli.
4. Manipulasi Tautan (Link). Manipulasi tautan adalah teknik di mana phisher mengirim tautan ke sebuah situs web. Saat pengguna mengklik tautan, itu membuka situs web phishing alih-alih tautan situs web yang sebenarnya.

Konsekuensi dari kejadian ini adalah kerugian yang dialami oleh nasabah dan bank, karena informasi pribadi, termasuk akses login situs web, mungkin dapat diakses oleh pihak lain. Meskipun peretas tidak memperoleh keuntungan material dari tindakan ini, bank akan menghadapi berkurangnya kepercayaan dari pelanggan. Kasus di atas dapat diinterpretasikan sebagai pelanggaran yang diatur dalam Pasal 378 KUHP mengenai tindak pidana penipuan yang terkait dengan perolehan informasi pribadi (phishing) melalui pengiriman email, karena Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tidak mengatur secara spesifik mengenai phishing.

Perlindungan Hukum dan Pengaturan Hukum Terhadap Data Pribadi Nasabah Oleh Bank Dalam Transaksi Melalui Internet Banking

Menurut Pasal 1 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang dimaksud dengan data pribadi adalah sarana elektronik atau non-elektronik yang menyimpan data tentang dirinya dalam bentuk informasi pribadi. identitas atau informasi lain yang dapat diperoleh tentang dirinya. Selama penerapan online banking, jika ditemukan data pribadi nasabah bocor tanpa seizin nasabah, maka dapat dikatakan prinsip kerahasiaan bank belum diterapkan secara maksimal.[31] Pesatnya perkembangan teknologi membuat segala sesuatu yang dilakukan masyarakat mulai dari komunikasi hingga bisnis menjadi berbasis internet. Munculnya aplikasi berbasis Internet memudahkan kegiatan bisnis seperti Internet

[31] Elfian Fauzi and Nabila Alif Radika Shandy, "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Jurnal Lex Renaissance* 7, no. 3 (2022): 445–61, https://doi.org/10.20885/jlr.vol7.iss3.art1.

banking. Aspek yang menjadikan layanan perbankan begitu penting adalah kenyamanan. Namun saat menerapkannya, Anda perlu memperkuat postur keamanan Anda, jika tidak maka dapat menimbulkan masalah di kemudian hari dan menimbulkan keluhan pelanggan. Sesuai Pasal 1 POJK Nomor 18 /POJK 07/2018 tentang Pelayanan Pengaduan Konsumen Sektor Jasa Keuangan, penyampaian keluhan atau protes nasabah mengenai ketidakpuasan nasabah terhadap penggunaan fasilitas dan kerugian yang serius dilakukan secara tertulis atau Anda telah mengajukan keluhan lisan tentang kegagalan Layanan dalam memenuhi janjinya. Pengaduan dapat diterima dari pihak-pihak yang merupakan badan usaha. Salah satunya dengan melakukan transaksi perbankan berbasis internet banking.[32]

Tidak dapat disangkal bahwa kejahatan dunia maya juga berdampak pada nasabah bank. Meskipun bank merupakan salah satu lembaga keuangan yang memiliki protokol ketat, namun tidak dapat dipungkiri bahwa tindak pidana dapat terjadi dan pengaduan nasabah harus ditangani oleh bank sebagai penyedia jasa dan transaksi keuangan. Peraturan Bank Indonesia No. 10/10/PBI/2008 tentang Perubahan Atas Peraturan Bank Indonesia No. 7/7/PBI/2005 tentang Pengaduan Nasabah pada Pasal 2 ayat (1) dan (2) Peraturan Bank Indonesia Keputusan 10/10/PBI/2008 Tentang Keputusan Pengaduan Nasabah Bank Indonesia No.7/7/PBI/2005 Perubahan Peraturan No. mengatur bahwa seluruh nasabah harus bertanggung jawab kepada bank apabila pengaduan disampaikan oleh atau atas nama nasabah, ketetapan tersebut wajib dimiliki bank secara prosedur tertulis. Secara khusus, hingga saat ini belum terdapat undang-undang yang secara spesifik mengatur tentang internet banking. Namun, jika kita hubungkan dengan disiplin ilmu hukum, setiap perbuatan yang mengakibatkan kerugian pada orang lain membuat pihak yang melakukan perbuatan itu bertanggung jawab dan wajib mengganti kerugian yang dialami oleh orang lain akibat perbuatannya. Konsep ini dikenal sebagai tanggung jawab kualitatif, yaitu tanggung jawab yang muncul karena seseorang memiliki kualitas tertentu.

[32] Ni Putu Denisya, I Nyoman Putu Budiartha, and I Made Aditya Mantara Putra, "Perlindungan Hukum Terhadap Data Pribadi Nasabah Oleh Bank Dalam Transaksi Melalui Internet Banking," *Jurnal Preferensi Hukum* 5, no. 2 (2024): 246–52, https://doi.org/10.22225/jph.5.2.8088.246-252.

Seorang konsumen yang mengalami kerugian adalah pihak bank yang berhubungan dengan nasabah, yang mana pelaku dalam usaha ini dapat mengajukan gugatan terhadap pihak yang menyebabkan kerugian. Bank memiliki tanggung jawab untuk memberikan kompensasi kepada nasabah yang menderita kerugian. Ketentuan mengenai kewajiban bank untuk bertanggung jawab atas dana nasabah dapat diacu dalam peraturan yang lebih rendah, yaitu Peraturan Bank Indonesia Nomor 16/1/2014 tentang Perlindungan Konsumen Jasa Sistem Pembayaran. Pada pasal 10 peraturan tersebut dinyatakan bahwa kewajiban yang harus dilaksanakan oleh Penyelenggara adalah bertanggung jawab sepenuhnya atas segala kendala atau masalah yang mungkin timbul akibat tindakan yang dilakukan oleh penyelenggara, sehingga konsumen dapat menikmati hak-haknya. perlindungan hukum represif diwujudkan melalui undang-undang perlindungan konsumen, yang menjadi dasar bagi pemenuhan hak-hak konsumen dalam penggunaan internet banking atau saat menghadapi permasalahan dalam layanannya.[33]

Pengaturan hukum terkait dengan kejahatan siber berupa phising sebelumnya diatur dalam Pasal 378 KUHP mengenai penipuan. Sebagaimana kita ketahui, phising secara umum merupakan tindakan penipuan. Definisi penipuan yang dirumuskan dalam Pasal 378 KUHP adalah sebagai berikut:

> "Barang siapa yang dengan niat untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, menggunakan nama palsu atau identitas yang tidak benar, dengan tipu muslihat, atau serangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang, memberikan pinjaman, atau menghapuskan piutang, dapat dikenakan ancaman pidana penjara dengan maksimum hukuman selama empat tahun".

Berdasarkan elemen-elemen yang telah diuraikan dalam Pasal 378 KUHP, dapat disimpulkan bahwa subjek yang dimaksud adalah pelaku yang melakukan tindak pidana penipuan. Terdapat niat untuk menguntungkan diri sendiri atau orang lain, yang menunjukkan adanya

[33] Herdi Setiawan, Mohammad Ghufron, and Dewi Astutty Mochtar, "Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi E-Commerce," *MLJ Merdeka Law Journal* 1, no. 2 (2020): 102–11, https://doi.org/10.26905/mlj.v2i1.5496.

suatu kesengajaan yang dilakukan sebagai maksud (oogmerk).[34] Selanjutnya, perbuatan tersebut dilakukan secara melawan hukum, yang mengindikasikan bahwa pelaku penipuan tidak memiliki hak sama sekali untuk menikmati keuntungan yang diperoleh dari hasil penipuan tersebut. Selanjutnya, pelaku penipuan menggunakan nama palsu yang tentu saja dikenal baik oleh korban. Mereka mengangkat martabat palsu, misalnya dengan mengaku sebagai seorang kiai, dan melakukan tipu muslihat dengan berjanji akan membelikan barang dengan harga sangat murah bagi korban. Dalam rangkaian kebohongan ini, pelaku berusaha menipu dengan cara menceritakan bahwa mereka memiliki hubungan dekat dengan seseorang, di mana orang tersebut memiliki urusan dengan si korban. Kemudian, pelaku meminta uang dari korban untuk diserahkan kepada orang yang akan ditemui korban, dengan harapan korban memberikan uang tersebut kepada pelaku agar pelaku dapat menyerahkannya kepada orang yang memiliki urusan dengan si korban.[35]

Menggerakkan orang lain dapat diartikan sebagai tindakan di mana pelaku penipuan berupaya membuat orang yang ditipu melakukan apa yang diinginkannya, yaitu dengan menyerahkan suatu barang kepada pelaku. Memberi utang atau menghapus piutang menjadi bagian inti dari delik penipuan, di mana objek yang terlibat dapat berupa hak, seperti menciptakan utang atau menghapus piutang. Menurut Nico Keijzer, pasal yang paling relevan untuk tindakan orang yang memanipulasi komputer demi mendapatkan keuntungan adalah Pasal 378, karena mencakup hak. Namun, pasal ini tidak memenuhi unsur mengenai informasi elektronik dan/atau dokumen elektronik yang salah, sehingga Pasal 378 sebenarnya tidak tepat untuk diterapkan pada kejahatan siber dalam bentuk phishing.[36] Kasus phishing melalui pengiriman file APK termasuk dalam kategori tindak kejahatan pidana,

[34] Ardi Saputra Gulo, Sahuri Lasmadi, and Khabib Nawawi, "Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik," *PAMPAS: Journal of Criminal Law* 1, no. 2 (2021): 68–81, https://doi.org/10.22437/pampas.v1i2.9574.

[35] Sumardi Efendi, "Sanksi Kejahatan Penipuan Dengan Identitas Palsu Dalam Kuhp Indonesia Dan Fiqh Jinayah," *Jurnal Syari'ah Dan Peradilan Islam* 1, no. 2 (2021): 32–55.

[36] Aura Nasha Ramadhanti et al., "Cara Operasi Kejahatan Phising Di Ranah Siber Yang Diatur Oleh Positif Indonesia," *Jurnal Pendidikan Tambusai* 8, no. 1 (2024): 1299–1305.

namun pengaturan hukum terkait kasus phishing ini menggunakan UU ITE. Hal ini disebabkan karena Indonesia mengedepankan asas yang berbunyi *"lex specialis derogat legi generali"*. Asas tersebut mengandung makna bahwa jika terjadi suatu peristiwa yang bersifat spesial atau khusus, maka peraturan perundang-undangan yang digunakan harus sesuai dengan peristiwa tersebut agar lebih efektif dalam pelaksanaannya.

Meskipun Indonesia mengikuti prinsip tersebut dan menerapkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai regulasi yang secara khusus membahas kejahatan-kejahatan siber seperti phishing, jika kita meneliti ketentuan-ketentuan yang ada di dalam UU ITE, kita menemukan bahwa tidak terdapat pasal-pasal yang memenuhi unsur-unsur phishing, melainkan hanya mendekati unsur tersebut. Hal ini dapat menimbulkan ketidakpastian hukum dalam penerapannya.[37] Kasus phishing termasuk dalam kategori kejahatan siber atau cybercrime, sehingga dalam pengaturan hukumnya digunakan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, karena undang-undang ini memiliki sifat "khusus" yang diterapkan untuk mengatur penggunaan teknologi di Indonesia. Meskipun UU ITE tidak menjelaskan secara jelas mengenai phishing, terdapat beberapa pasal yang dianggap dapat menjadi payung hukum untuk kasus phishing, yaitu Pasal 35. Berikut adalah penjelasan mengenai pasal tersebut:

Kelemahan Regulasi dan Urgensi Reformulasi Hukum dalam Menangani Phishing Berbasis File APK di Indonesia

Pasal 35 UU ITE mengatur bahwa tidak diperbolehkannya melakukan manipulasi atau penciptaan suatu informasi elektronik atau dokumen elektronik dengan tujuan agar informasi atau dokumen elektronik tersebut dianggap sebagai data asli atau otentik. Bunyi pasal tersebut dapat dikaitkan dengan kasus phishing melalui file apk. Unsur

[37] Artanti Zahra Adisa and Andriyanto Adhi Nugroho, "Perlindungan Hukum Terhadap Korban Phising Terkait Pengiriman File Apk," *Justisi* 10, no. 1 (2024): 242–56, https://doi.org/10.33506/js.v10i1.2980.

"setiap orang" dalam hal ini merujuk pada phisher yang dengan sengaja dan tanpa haknya memanipulasi file berbentuk apk dengan memberikan nama untuk file tersebut seolah-olah dokumen penting (seperti foto paket yang akan dikirimkan, undangan pernikahan, atau surat tilang elektronik). Penjatuhan hukuman dari Pasal 35 merujuk pada ketentuan Pasal 51, yaitu dengan penjatuhan hukuman penjara yang dapat berlangsung paling lama 12 (dua belas) tahun dan/atau dikenakan denda paling banyak Rp12. 000. 000. 000,00 (dua belas miliar rupiah).

Berdasarkan pasal Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik serta Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (yang selanjutnya disingkat dengan UU ITE) yang kiranya relevan untuk kasus phishing melalui pengiriman file berformat apk, pasal-pasal tersebut memberikan hukuman dalam bentuk hukuman pidana pokok baik berupa pidana penjara maupun pidana denda sebagai mana yang tercantum dalam KUHP. Namun kenyataannya, pasal-pasal tersebut masih belum cukup memenuhi unsur-unsur yang ada pada kasus phishing. Contohnya, seperti yang dapat dilihat dari isi Pasal 35 UU ITE. Isi Pasal 35 UU ITE tersebut memiliki unsur-unsur yang paling memenuhi konsep phishing itu sendiri, tetapi beberapa unsur phishing tidak terdapat di dalam pasal tersebut sehingga menyebabkan Pasal 34 mengalami kebingungan norma karena tidak memiliki konsep yang jelas terkait phishing itu sendiri.[38] Kemudian, jika pelaku phishing atau phisher dalam aksinya juga mengambil data pribadi milik korban, contohnya seperti informasi terkait kesehatan korban, data-data biometrik yang terdapat di dalam perangkat milik korban, dan lainnya di samping phisher tersebut mengambil peluang yang terdapat di dalam rekening m-banking korban, maka phisher tersebut dapat dikenakan hukuman berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Namun, UU PDP hanya sebatas memberikan pengaturan terkait pencurian data pribadi

[38] Septian Arya Budi Mahesa, "Optimalisasi Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dalam Penanganan Perkara Tindak Pidana Phising," *COMSERVA Indonesian Jurnal of Community Services and Development* 2, no. 11 (2023): 2686–96, https://doi.org/10.59141/comserva.v2i11.670.

saja seperti yang tercantum dalam Pasal 67 Ayat (1) UU PDP, dan hal tersebut kurang relevan jika dikenakan untuk kasus phishing melalui pengiriman file berformatkan apk.

Indonesia memiliki urgensi untuk menambah atau mengubah pasal-pasal yang sudah ada dengan memasukkan unsur-unsur yang berkaitan dengan konsep phishing atau membentuk suatu regulasi perundang-undangan yang baru secara khusus membahas mengenai phishing, mengingat kasus-kasus phishing di Indonesia masih banyak terjadi. Selain itu, diperlukan juga sosialisasi yang dilakukan secara berkala dan merata terhadap seluruh masyarakat di Indonesia terkait ancaman siber, salah satunya adalah phishing melalui pengiriman file, dan upaya penanggulangan jika sudah terlanjur mengklik file tersebut.

Implikasi Phishing Terhad ap Privasi Pengguna

Warren dan Brandheis dalam karya ilmiah bertajuk "The Right to Privacy" mendefinisikan privasi sebagai hak yang dimiliki oleh setiap individu untuk menikmati dan menjaga privasinya. Prinsip hak atas privasi berkenaan dengan data pribadi bertujuan untuk melindungi individu dari tindakan kejahatan yang bersifat melanggar etika dan kejujuran dalam pelaksanaannya.[39] Hak atas privasi ini mencakup hak setiap individu untuk memiliki kontrol penuh mengenai informasi yang berkaitan dengan data mereka, termasuk mengetahui apa yang terjadi dengan data tersebut, siapa yang diizinkan untuk mengaksesnya, bagaimana data itu didistribusikan, serta untuk tujuan apa data tersebut digunakan. Perlindungan hukum terkait privasi dan data pribadi juga dianggap penting di negara lain, seperti yang diatur dalam beberapa pedoman Uni Eropa (Directive), yang membedakan antara kategori data sensitif dan non-sensitif berdasarkan tingkat risiko yang mungkin dihadapi individu jika data tersebut diakses oleh pihak-pihak yang tidak bertanggung jawab.[40]

Dampak dari phishing sangatlah merugikan dan dapat terjadi dalam berbagai bentuk. Salah satunya adalah kehilangan uang dalam

[39] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy* (Boston: Lawrence University, n.d.), https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

[40] Ilfa Sholikhah Hendarto, "Implikasi Pengaruh Minimnya Pengaturan Perlindungan Privasi Data Pribadi Nasabah Pada Perbankan Digital," *Journal Justiciabelen (JJ)* 4, no. 02 (2024): 129, https://doi.org/10.35194/jj.v4i02.4440.

jumlah yang signifikan. Penipu memiliki kemampuan untuk mengakses akun keuangan korban dan melakukan transaksi yang ilegal.[41] Di samping itu, informasi pribadi yang berhasil dicuri dapat disalahgunakan untuk berbagai tujuan jahat, seperti penipuan identitas atau pencurian data. Tidak jarang, korban phishing juga merasakan stres dan kecemasan akibat pelanggaran privasi yang mereka alami.[42] Oleh karena itu, sangat penting bagi kita untuk selalu waspada dan menerapkan langkah-langkah keamanan yang sesuai untuk melindungi diri. Selain itu, individu juga berisiko mengalami pencurian identitas yaitu penyalahgunaan data pribadi: informasi pribadi seperti nama lengkap, alamat, nomor telepon, dan nomor KTP yang berhasil dicuri dapat disalahgunakan oleh pelaku kejahatan untuk melakukan berbagai tindakan ilegal, seperti membuka rekening bank baru atau mengajukan pinjaman atas nama korban, kerugian finansial: akibat pencurian identitas, korban dapat mengalami kerugian finansial yang cukup besar. Misalnya, tagihan kartu kredit yang tidak diakui atau penipuan online yang dapat mengakibatkan informasi pribadi mereka jatuh ke tangan orang yang tidak bertanggung jawab. Phishing juga dapat merusak perangkat smartphone atau komputer akibat infeksi malware (malicious software). Kejadian ini berpotensi menurunkan kepercayaan pelanggan dan mengancam reputasi perusahaan dalam jangka panjang terhadap layanan online yang mereka gunakan akibatnya korban mungkin enggan untuk menggunakan layanan online lainnya, meskipun layanan tersebut sebenarnya aman, misalnya akun yang telah diambil alih oleh pelaku dapat digunakan untuk melakukan tindakan yang merugikan orang lain, seperti menyebarkan ujaran kebencian atau melakukan penipuan dan kerusakan reputasi akibat phising sangat sulit untuk dipulihkan, bahkan setelah akun berhasil diambil alih kembali. Dampak lainnya adanya akses ilegal ke akun pribadi dengan mendapatkan kata sandi dan informasi login, pelaku dapat mengakses berbagai akun pribadi korban, seperti email, media sosial, dan akun perbankan. Informasi pribadi yang ada di dalam akun tersebut dapat disebarluaskan secara bebas oleh

[41] Faiz Emery Muhammad and Beniharmoni Harefa, "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web," *Jurnal Usm Law Review* 6, no. 1 (2023): 226, https://doi.org/10.26623/julr.v6i1.6649.

[42] Leticia M. Malunsenge, Cornelis Dj. Massie, and Ronald E. Rorie, "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising Di Indonesia," *Lex Crimen*, 2022.

pelaku, sehingga menyebabkan reputasi korban rusak.[43]

Penutup

Phishing adalah jenis serangan siber yang memanfaatkan teknik manipulasi atau penipuan untuk mendapatkan informasi pribadi secara ilegal. Pelaku phishing biasanya menyamar sebagai orang atau lembaga yang terpercaya, seperti bank, perusahaan, atau bahkan teman atau keluarga, untuk menipu korban agar memberikan informasi sensitif seperti kata sandi, nomor rekening, atau data kartu kredit. Hasil kajian dalam penelitian ini, ditemukan bahwa phishing di Indonesia menunjukkan pola yang semakin kompleks dan canggih, terutama melalui media berbasis aplikasi (seperti file APK), media sosial, serta website palsu yang meniru situs resmi lembaga keuangan. Kasus phishing terhadap layanan KlikBCA pada 2001 menjadi titik awal kesadaran akan perlunya regulasi hukum di ranah digital. Sejak itu, kasus phishing telah berkembang dalam skala dan teknik, menyasar sektor-sektor vital seperti perbankan, e-commerce, dan layanan pemerintah. Namun, secara normatif, Indonesia masih menghadapi kendala serius dalam hal efektivitas regulasi. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) memang memuat beberapa ketentuan yang relevan, seperti Pasal 35, namun tidak secara spesifik merumuskan unsur-unsur tindak pidana phishing. Hal ini menyebabkan ketidaktepatan penegakan hukum karena adanya kekosongan norma atau *legal gap*. Di sisi lain, Undang-Undang Perlindungan Data Pribadi (UU PDP) memberikan dasar hukum terkait pencurian data, tetapi tidak cukup untuk menjerat pelaku phishing yang juga melakukan manipulasi dan rekayasa sosial.

Kelemahan regulasi ini berdampak langsung terhadap jaminan perlindungan hak atas privasi digital pengguna. Meskipun prinsip-prinsip perlindungan privasi telah dijelaskan dalam berbagai instrumen hukum nasional dan internasional, implementasinya di Indonesia masih lemah, baik dari segi penegakan hukum, kapabilitas lembaga penegak hukum, maupun dari sisi literasi digital masyarakat. Berdasarkan temuan penelitian ini, disarankan agar pemerintah Indonesia segera merumuskan regulasi khusus yang secara eksplisit mengatur dan

[43] Luh Intan Candhika Dharani, Soesi Idayanti, and Kanti Rahayu, *Perlindungan Hukum Terhadap Tindakan Phishing Di Media Sosial* (Pekalongan: Penerbit NEM, 2024).

mengkriminalisasi tindak phishing, mengingat ketidakjelasan norma dalam UU ITE dan keterbatasan cakupan UU PDP dalam menjangkau kompleksitas modus kejahatan siber berbasis manipulasi data. Selain itu, diperlukan penguatan kelembagaan penegakan hukum terkait perlindungan data pribadi, peningkatan literasi digital masyarakat, serta pembentukan sistem tanggap darurat yang efektif terhadap insiden phishing. Meski demikian, penelitian ini memiliki keterbatasan pada pendekatan yuridis-normatif yang lebih menitikberatkan pada studi pustaka dan analisis dokumen hukum tanpa mengikutsertakan data empiris secara langsung dari pelaku, korban, maupun aparat penegak hukum. Oleh karena itu, studi lanjutan dengan pendekatan empiris dan interdisipliner sangat dibutuhkan guna memperkaya pemahaman dan mengembangkan rekomendasi kebijakan yang lebih komprehensif dan kontekstual.

Daftar Pustaka

Abdullah, Varatisha. "SOSIAL MEDIA SEBAGAI PASAR BAGI MASYARAKAT MODERN (Sebuah Kritik Terhadap Budaya Populer)." *Jurnal Dakwah Tabligh* 18, no. 1 (2017): 1–15. https://doi.org/10.24252/jdt.v18n1dnk02.

Affeldt, Fabrício Sobrosa, and Sady Darcy da Silva Junior. "Information Architecture Analysis Using Business Intelligence Tools Based on the Information Needs of Executives." *Journal of Information Systems and Technology Management* 10, no. 2 (2013): 251–70. https://doi.org/10.4301/s1807-17752013000200004.

Anderson, Ross, Chris Barton, Rainer B¨ohme, Richard Clayton, Carlos Ga˜n´an, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. "Measuring the Changing Cost of Cybercrime." In *Workshop on the Economics of Information Security*, 2019. https://doi.org/https://doi.org/10.17863/CAM.41598.

Artanti Zahra Adisa, and Andriyanto Adhi Nugroho. "Perlindungan Hukum Terhadap Korban Phising Terkait Pengiriman File Apk." *Justisi* 10, no. 1 (2024): 242–56. https://doi.org/10.33506/js.v10i1.2980.

Arya Budi Mahesa, Septian. "Optimalisasi Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dalam Penanganan Perkara Tindak Pidana Phising." *COMSERVA Indonesian Jurnal of Community Services and Development* 2, no. 11 (2023): 2686–96. https://doi.org/10.59141/comserva.v2i11.670.

Bhavsar, Vaishnavi, Aditya Kadlak, and Shabnam Sharma. "Study on Phishing Attacks." *International Journal of Computer Applications* 182, no. 33 (2018): 27–29. https://doi.org/10.5120/ijca2018918286.

Brandao, Pedro Ramos, and Henrique S Mamede. "Phishing and Advanced Persistent Threats." *Journal of Mathematical & Computer Applications*, 2022, 1–4. https://doi.org/10.47363/jmca/2022(1)105.

Bruce, Miranda, Jonathan Lusthaus, Ridhi Kashyap, Nigel Phair, and Federico Varese. "Mapping the Global Geography of Cybercrime with the World Cybercrime Index." *PLoS ONE* 19, no. 4 April (2024). https://doi.org/10.1371/journal.pone.0297312.

Caniago, Koko, and Tata Sutabri. "Tindak Kejahatan Phising Di Sektor Pelayanan Di Universitas Bina Insan Lubuklinggau." *Jurnal Riset Sistem Informasi Dan Teknik Informasi* 8, no. 1 (2023): 117–25.

Denisya, Ni Putu, I Nyoman Putu Budiartha, and I Made Aditya Mantara Putra. "Perlindungan Hukum Terhadap Data Pribadi Nasabah Oleh Bank Dalam Transaksi Melalui Internet Banking." *Jurnal Preferensi Hukum* 5, no. 2 (2024): 246–52. https://doi.org/10.22225/jph.5.2.8088.246-252.

Desai, C, and V P Desai. "Ensuring Data Security in Human Resource Management: Importance, Challenges \&Techniques." In *Sdmimd.Ac.In*, n.d. https://www.sdmimd.ac.in/conferenceproceedings/ihr2024papers/IHR2418.pdf.

Dharani, Luh Intan Candhika, Soesi Idayanti, and Kanti Rahayu. *Perlindungan Hukum Terhadap Tindakan Phishing Di Media Sosial*. Pekalongan: Penerbit NEM, 2024.

Dm, Mohd Yusuf, Addermi, and Jasmine Lim. "Kejahatan Phising Dalam Dunia Cyber Crime Dan Sistem Hukum Di Indonesia." *Jurnal Pendidikan Dan Konseling* 4, no. 5 (2022): 8018–23.

Efendi, Sumardi. "Sanksi Kejahatan Penipuan Dengan Identitas Palsu Dalam Kuhp Indonesia Dan Fiqh Jinayah." *Jurnal Syari'ah Dan Peradilan Islam* 1, no. 2 (2021): 32–55.

Fauzi, Elfian, and Nabila Alif Radika Shandy. "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Jurnal Lex Renaissance* 7, no. 3 (2022): 445–61. https://doi.org/10.20885/jlr.vol7.iss3.art1.

Grabosky, Peter. *Cybercrime*. Edited by Henry N. Pontell. Oxford University Press, 2015.

Gulo, Ardi Saputra, Sahuri Lasmadi, and Khabib Nawawi. "Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik." *PAMPAS: Journal of Criminal Law* 1, no. 2 (2021): 68–81. https://doi.org/10.22437/pampas.v1i2.9574.

Harahap, Handika Saputra, Alif Allegra Rahman, Indah Suraswati, and Shelvie Nidya Neyman. "Memahami Cara Kerja Phishing Menggunakan Tools Pada Kali Linux." *Journal of Internet and Software Engineering* 1 (2024): 1–11.

Haryanto, Agus Tri. "APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang." detiknet, 2024. https://inet.detik.com/cyberlife/d-7169749/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang.

Hendarto, Ilfa Sholikhah. "Implikasi Pengaruh Minimnya Pengaturan Perlindungan Privasi Data Pribadi Nasabah Pada Perbankan Digital." *Journal Justiciabelen (JJ)* 4, no. 02 (2024): 129. https://doi.org/10.35194/jj.v4i02.4440.

Holivia, Anjeli, and Teguh Suratman. "Child Cyber Grooming Sebagai Bentuk Modus Baru Cyber Space Crimes." *Bhirawa Law Journal* 2, no. 1 (2021): 1–13. https://doi.org/10.26905/blj.v2i1.5847.

Leticia M. Malunsenge, Cornelis Dj. Massie, and Ronald E. Rorie. "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising Di Indonesia." *Lex Crimen*, 2022.

Levy, Adam. *Avoiding the Ransom Cybersecurity for Business Owners and Managers*. Magnet Solution Group Press, 2016.

Lubbad, Anas R M. "Information Technology Readiness and the Assessment and Adoption of Information Technology Innovativeness." *Advances in Life Science and Technology*, 2021. https://doi.org/10.7176/alst/90-04.

Ludwianto, Bianda. "91 Juta Data Pengguna Tokopedia Yang Bocor Beredar Gratis Di Facebook," 2020. https://kumparan.com/kumparantech/91-juta-data-pengguna-tokopedia-yang-bocor-beredar-gratis-di-facebook-1tkItz2vI05?

Manglik, Rohit. *Cybercrime, Law and Countermeasures*. EduGorilla Publication, 2024.

Maskun. *Kejahatan Siber Cybercrime: Suatu Pengantar*. Jakarta: Kencana, 2013.

Muftiadi A, Putri Mulyani Agustina T, and Evi M. "Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phising Terhadap Layanan Online Banking." *HEXATECH Jurnal Ilmiah Teknik* 1 (2022).

Muhammad, Faiz Emery, and Beniharmoni Harefa. "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web." *Jurnal Usm Law Review* 6, no. 1 (2023): 226. https://doi.org/10.26623/julr.v6i1.6649.

Phishing.org. "History of Phishing." Accessed March 15, 2025. https://www.phishing.org/history-of-phishing?

Poudel, Bishal, and Satish Kumar Karna. "What Influences a Hacker to Be a Black Hat?" *Medicon Engineering Themes*, 2024. https://doi.org/10.55162/mcet.06.215.

Pranata, Eko Jhony, and Lukman Ependi. "Phising Terhadap Website Bank Bca." *Jurnal Trends* 01, no. 01 (2023): 34–40. https://ejurnal.ibisa.ac.id/index.php/jsd/article/view/293.

Radya Dzuhrizha Rahmana, Adhitya Widya Kartika. "Penegakan Hukum Bagi Pelaku Pembuatan Dan Penyebaran Scam Page (Studi Di Kepolisian Daerah Jawa Timur)." *Risalah Hukum* 2 (2022): 83–98.

Ramadhanti, Aura Nasha, Tessa Ayuning Tias, Erin Dwi Lestari, and Asmak UI Hosnah. "Cara Operasi Kejahatan Phising Di Ranah

Siber Yang Diatur Oleh Positif Indonesia." *Jurnal Pendidikan Tambusai* 8, no. 1 (2024): 1299–1305.

Sari, Rita Puspita. "RI Masuk 10 Besar Kebocoran Data, Hampir 100 Juta Akun Bocor," 2024. https://csirt.or.id/berita/ri-masuk-10-besar-kebocoran-data?

Setiawan, Herdi, Mohammad Ghufron, and Dewi Astutty Mochtar. "Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi E-Commerce." *MLJ Merdeka Law Journal* 1, no. 2 (2020): 102–11. https://doi.org/10.26905/mlj.v2i1.5496.

Sinaga, Oriza, Lucysera, Khodijah Ismail, Dimas Syahpura, and Amalia Pitri. "Pengaruh Perkembangan Teknologi Terhadap Pola Komunikasi Masyarakat." *JURNAL SIMBOLIKA Research and Learning in Comunication* 4, no. 2 (2021): 188–99. https://www.researchgate.net/publication/348408331_Pengaruh_Perkembangan_Teknologi_Terhadap_Pola_Komunikasi_Masyarakat.

Steinmetz, Kevin F., Brian P. Schaefer, Adrienne L. McCarthy, Christopher G. Brewer, and Don L. Kurtz. "Exploring Cybercrime Capabilities: Variations Among Cybercrime Investigative Units." *Criminal Justice Policy Review* 35, no. 4 (2024): 194–215. https://doi.org/10.1177/08874034241265106.

Teo, Thompson S.H. "Differential Effects of Occupation on Internet Usage." *Internet Research* 8, no. 2 (1998): 156–65. https://doi.org/10.1108/10662249810211629.

Wall, David S. "Cybercrime: The Transformation of Crime in the Information Age, 2nd Edition, Cambridge: Polity (Outline of Update)." *SSRN Electronic Journal*, 2024. https://doi.org/10.2139/ssrn.4707509.

Warren, Samuel D., and Louis D. Brandeis. *The Right to Privacy*. Boston: Lawrence University, n.d. https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

Yuspin, Wardah, Alda Oktalivia Putri, Ata Fauzie, and Jompon Pitaksantayothin. "Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities."

International Journal of Safety and Security Engineering 14, no. 6 (2024). https://doi.org/10.18280/ijsse.140605.

Zhipeng, Ye. "The Social Impact of the Evolution of Internet Language: A Critical Discourse Analysis of Popular Internet Language." *Lecture Notes on Language and Literature* 7, no. 2 (2024). https://doi.org/10.23977/langl.2024.070223.